

Use of Wireless Communications Devices in Voting Systems

David Cypher

NIST

TGDC Meeting, April 20 & 21, 2005

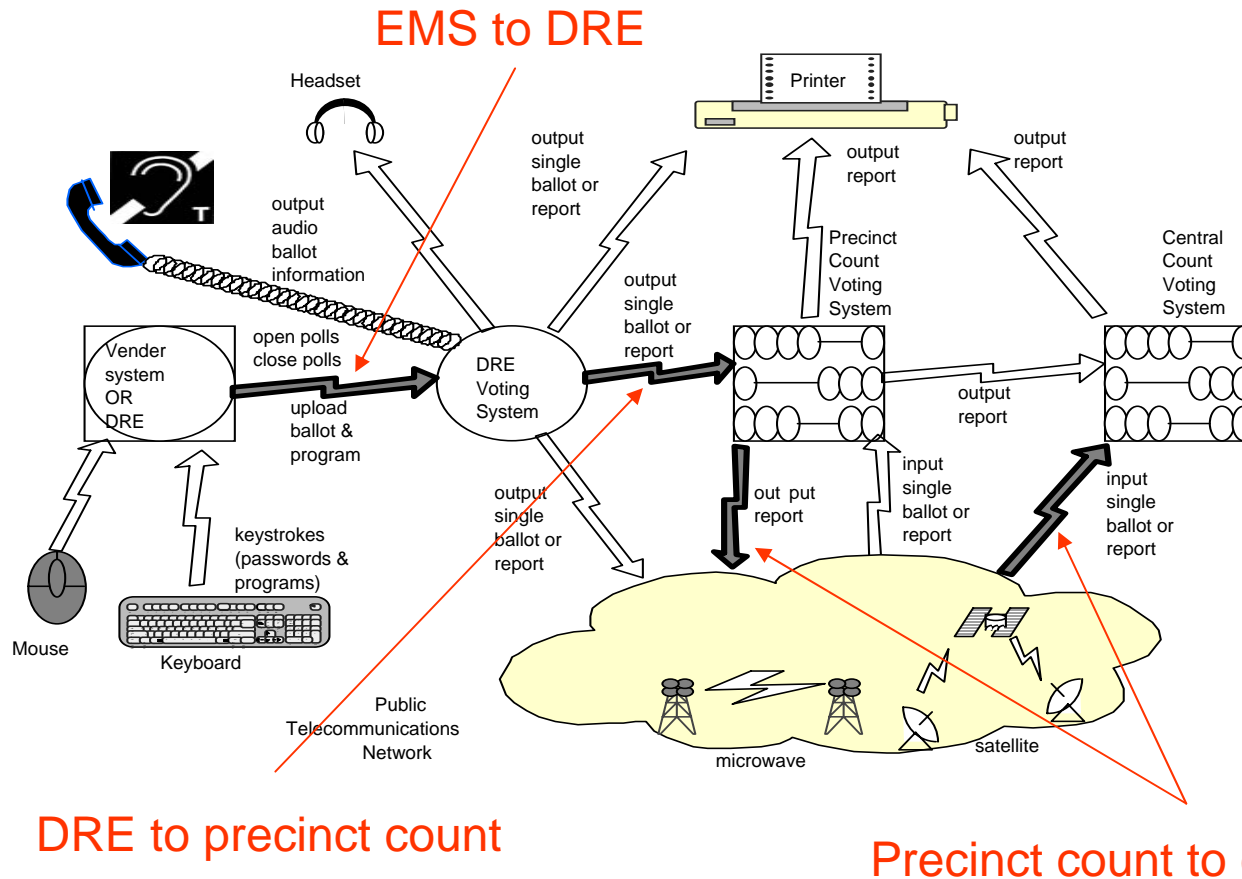
Goals

- To respond to the TGDC's resolution #35-05
 - by reaching a common understanding of the subject (wireless communications devices) by providing background information
 - by identifying technical requirements for the use of wireless communications devices

Progress

- Created draft requirements for the use of wireless communications for voting systems,
 - limited to investigate current implementations' wireless communication usage as directed by the TGDC from the March 9th, 2005 meeting.
- Most of the requirements are simply reemphasizing the existing requirements of the VSS 2002.

Existing wireless locations



Requirements Overview

- Apply telecommunications
- Information
 - Controlling usage
 - Identifying usage
 - Protecting transmitted data
 - Protecting the wireless path
- System
 - Protecting from wireless-based attacks

Controlling usage

- security documentation
 - Cryptographic key management, public or recognized expert review
- able to operate without wireless
- wireless on/off capability
- wireless not on automatically
- Radio Frequency
 - Proper selection from numerous choices
 - Signal strength control
 - Radio emission site test

Identifying usage

- Method for determining existence of wireless
- Method for determining activity of wireless
 - Visual indication
- Labeling of wireless

Protecting transmitted data

- Encryption and authentication
 - FIPS 197
 - FIPS140-2
- Only exception
 - Exception for wireless coupling audible

Protecting the wireless path

- Assume infinite duration of Denial of Service (DoS)
- Assume wireless is never available
- Alternatives
 - Procedures
 - Capabilities
- Audible shall be protected
- Infrared shall be protected for short distances

System (Protecting from wireless-based attacks)

- Existing security VSS 2002 section 2.2.1
- Existing accuracy VSS 2002 section 2.2.2
 - Additional concern caused by wireless
- Existing error recovery VSS 2002 section 2.2.3
- Logging
 - System audit VSS 2002 section 2.2.5
 - Integrity VSS 2002 section 2.2.4
 - Log items
- Authentication
 - Device
 - User

The technology (wireless) is ever evolving as is its security.
Therefore its use a perpetual risk needing to be evaluated.